State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory

July 22, 2016

The following cyber advisory was issued by the State of Alaska and
was intended for State government entities. The information may or
may not be applicable to the general public and accordingly, the State
does not warrant its use for any specific purposes.

ADVISORY NUMBER:
SA2016-109

DATE(S) ISSUED:
07/21/2016

SUBJECT:
Multiple Vulnerabilities in Google Chrome Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Google Chrome, the most severe of
which could result in remote code execution. Google Chrome is a web browser used to
access the Internet. These vulnerabilities can be exploited if a user visits, or is redirected
to, a specially crafted web page. Successful exploitation of these vulnerabilities could
allow an attacker to execute remote code in the context of the browser, obtain sensitive
information, bypass security restrictions, or cause denial-of-service conditions.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:
  · Google Chrome prior to 52.0.2743.82

RISK:
Government:
  · Large and medium government entities: **High**
  · Small government entities: **Medium**
Businesses:
  · Large and medium business entities: **High**
  · Small business entities: **Medium**
Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Google Chrome, the most severe of
which could result in remote code execution. These vulnerabilities can be exploited if a

user visits, or is redirected to, a specially crafted web page. Details of the vulnerabilities are as follows:

- · Sandbox escape in PPAI (CVE-2016-1706)
- · URL spoofing in iOS (CVE-2016-1707)
- · Use-after-free in Extensions (CVE-2016-1708)
- · Heap-based buffer-overflow that exists in sfntly (CVE-2016-1709)
- · Same-origin bypass in Blink. (CVE-2016-1710, CVE-2016-1711)
- · Use-after-free error in Blink. (CVE-2016-5127)
- · Same-origin bypass in V8. (CVE-2016-5128)
- · Memory corruption vulnerability that exists in V8. (CVE-2016-5129)
- · URL spoofing error. (CVE-2016-5130)
- · Use-after-free error in libxml. (CVE-2016-5131)
- · Limited same-origin bypass error in Service Workers. (CVE-2016-5132)
- · Origin confusion error in proxy authentication. (CVE-2016-5133)
- · Information-disclosure vulnerability that exists due to URL leakage through PAC script. (CVE-2016-5134)
- · Content security-policy bypass. (CVE-2016-5135)
- · Use-after-free error in extensions. (CVE-2016-5136)
- · Information-disclosure vulnerability that exists due to history sniffing with HSTS and CSP. (CVE-2016-5137)
- · Multiple unspecified security vulnerabilities. (CVE-2016-1705)

Successful exploitation of these vulnerabilities could allow an attacker to execute remote code in the context of the browser, obtain sensitive information, bypass security restrictions, or cause denial-of-service conditions.

RECOMMENDATIONS:
We recommend the following actions be taken:
- · Apply appropriate patches provided by Google to vulnerable systems immediately after appropriate testing.
- · Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- · Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- · Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:
Google:
http://googlechromereleases.blogspot.in/2016/07/stable-channel-update.html

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1705
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1706
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1707
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1708
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1709
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1710
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1711
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5127
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5128
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5129
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5130
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5131
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5132
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5133

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5134
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5135
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5136
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5137